ATTORNEY DOCKET NO. BOE01 003

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DESIGNATED OFFICE

In re the Application of: Robert Frischholz

International Application No.: PCT/EP00/00367

International Filing Date: January 18, 2000

Priority Date Claimed: January 19, 1999

Title: A METHOD AND SYSTEM OF SECURING FORGERY IN BIOMETRICAL IDENTIFICATION OF PERSONS

TRANSMITTAL

United States Designated Office
United States Patent and Trademark Office
Box PCT
Washington, D.C. 20231

Sir:

Please commence national stage examination pursuant to 35 U.S.C. 371 for the above-identified PCT patent application.

Enclosed are:

[X] A copy of the international application as filed, including:

[X] Abstract, 9 pages of specification and Claim(s) 1-18.

[X] Two (2) sheets of formal drawings showing Figures 1-2.

[X] An English Translation of the application as filed including:

[X] Abstract, 9 pages of specification and Claims(s) 1-18.

[X] Two (2) sheets of informal drawings showing Figures 1-2.

[X] The International Preliminary Examination Report.

[X] An International Search Report from the EPO.

[X] An English Translation of the Annex to an International Preliminary Examination Report.

[X] A Preliminary Amendment canceling Claims 7-18 and adding Claims 19-31.

[X] A check in the amount of $860.00 to cover the filing fee as calculated below:

NUMBER OF CLAIMS		NUMBER EXTRA		LARGE/SMALL ENTITY	FEE
TOTAL	19 - 20 =	0	x	$18 or $9 =	$ 0
INDEP.	2 - 3 =	0	x	$80 or $40 =	$ 0
MULTIPLE DEPEND.	[ ] Yes			$270 or $135 =	$ 0
For filing with EPO or JPO search report				$860 or $430 =	$860.00
If International Preliminary Exam fee paid to USPTO				$690 or $345 =	$
If International Preliminary Exam fee paid to USPTO and all USPTO indicates all claims are allowable				$ 100 or $ 50 =	$
If International Search fee paid to USPTO, but International Preliminary Exam fee not paid to USPTO				$710 or $355 =	$
If neither International Search fee nor International Preliminary Exam fee paid to USPTO				$1,000 or $500 =	$
				TOTAL FILING FEES =	$860.00

The Commissioner is hereby authorized to charge payment of any additional fees associated with this communication under 37 CFR 1.492 or CFR 1.16 or to credit any overpayment to Deposit Account No. 18-1835.

A duplicate of this sheet is enclosed.

Respectfully submitted,

L. Lawton Rogers, III
Reg. No. 24,302
D. Joseph English
Reg. No. 42,514
Mark C. Comtois
Reg. No. 46,285
Patrick D. McPherson
Reg. No. 46,255

1401 Eye Street, N.W., Suite 300
Washington, DC 20005
Telephone: (202) 898-1515
Telecopier: (202) 898-1521

Dated: July 19, 2001

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of Robert Frischolz

Serial No.: Unassigned

Filed: Herewith

International Application No.: PCT/EP00/00367

International Filing Date: January 18, 2000

Priority Date Claimed: January 19, 1999

Title: A METHOD AND SYSTEM OF SECURING FORGERY IN BIOMETRICAL IDENTIFICATION OF PERSONS

PRELIMINARY AMENDMENT

The Honorable Commissioner of
Patent and Trademarks
Washington, D.C. 20231

Sir:

Preliminary to the examination of the subject application, please amend the subject application as follows:

In the Claims:

Please cancel Claims 7-18 without prejudice.

Please add the following new Claims 19-31:

–19. (New) The method as claimed in claim 5, wherein an alarm is given if the motions do not follow the target directions repeatedly in succession.

–20. (New) The method as claimed in claim 6, wherein an alarm is given if the motions do not follow the target directions repeatedly in succession.

–21. (New) The method as claimed in claim 1, wherein a facial picture is taken of the person and digitized, and the actual position of the eyes in the digitized image is detected and compared with a rated eye position, and the digitized facial image is compared with at least one digital facial reference image if the actual eye position largely corresponds with the rated eye position.

–22. (New) The method as claimed in claim 1, wherein the picture of a hand print or finger print of the person is taken and digitized, the actual position of the picture in a detection area is determined and compared with a rated position, and the digitized image is com-pared with at least one digital reference image if the actual position largely corresponds with the rated position.

–23. (New) The method as claimed in claim 1, wherein the motion is detected before, after, or during the identification of the person.

–24. (New) A system of securing forgery in biometrical identification of persons, comprising a detector means for detecting at least one biological characteristic of a person and a processing means for transforming the characteristic detected into personal data, characterized by a directing means for releasing a certain motion of the person, the motion being detected by the detector means, wherein said processing means verifies whether the person is actually present in dependence of the detection result.

–25. (New) The system as claimed in claim 24, wherein the directing means comprises a monitor on which a mark is adapted to be displayed at random positions in order to direct the person's motion to that mark.

–26. (New) The system as claimed in claim 25, wherein the directing means controls the person's line of sight, the detector means detects the eye position, and the processing means digitizes the eye position detected and compares it with the rated eye position.

–27. (New) . The system as claimed in claim 24, wherein the directing means is part of the detector means.

–28. (New) The system as claimed in claim 27, wherein the detector means comprises a digitizing tray to control the person's hand motions and detect the position of the hand, and the processing means digitizes the hand position detected and compares it with a rated position.

–29. (New) The system as claimed in claim 28, wherein the detector detects a fingerprint of the person at the rated position only.

–30. (New) A method of biometrical identification of persons comprising a method as claimed in claim 1, wherein the person's data are compared with reference data.

-- 31. (New) A means for biometrical identification of persons, comprising a system as claimed in claim 24, wherein the processing means compares the person's data with reference data.

Respectfully submitted,

By: _____

L. Lawton Rogers, III
Reg. No. 24,302
D. Joseph English
Reg. No. 42,514
Mark C. Comtois
Reg. No. 46,285
Patrick D. McPherson
Reg. No. 46,255

1401 Eye Street, N.W., Suite 300
Washington, D.C. 20005
Telephone: (202) 898-1515
Telecopier: (202) 898-1521

Dated: July 19, 2001

DCS Dialog Communication Systems AG
D 2963 PCT

A method and system of securing forgery in biometrical identification of persons,

The invention relates to a method and a system of securing forgery in a biometrical identification of a person according to the preamble of claims 1 and 11, respectively. Such methods and systems are known from DE 44 13 788, U.S. 4,841 575 and U.S. 5,483,601.

Methods and systems of biometrical identification of persons are known which rely on a combination of facial recognition and recognition of lip movements. Such a method has been described, for example, in the applicant's German patent application 19 847 261 to which reference is made here. In personal recognition a distinction is made between the identification of one person among many others, i.e. answering the question: "Who is the person?" and the verification of a person, i.e. comparing the person's data with a certain data set or answering the question: "Is the person the one it purports to be?". The invention relates to the latter case.

Biometrical personal identification methods are thought to be especially reliable because they make use of characteristics which are specific to a person. And yet the biometrical identification of persons is not completely safeguarded against falsifications. A special risk are the so-called replay attacks with which the biometrical data set of a person is entered illegally into a system so that the identification system supposedly identifies the biometrical data of a person and, for instance, grants that person access to a protected area or enables execution of a particular transaction.

Methods of safeguarding personal access data likewise are known in the art. With these methods of protection it must be noted that a fundamental difference exists between the biometrical identification of a person and other customary protective mechanisms, such as the allocation of a secrete code or password. If a secrete code or password is misappropriated its abuse can be prevented by blocking and reissuing it. It is practically impossible, on the other hand, to assign a new biometrical access identity because by its very nature it is peculiar to a person. For example, if the data set of a finger is spied out wrongfully in a finger print system this characteristic of a person cannot be assigned anew. The same is true of a facial

recognition system because no other face can be used for identification of a person but the face of that very same person.

Nowadays, certain measures of security already are taken when the biometrical data of a person are recorded in order to ward off those kinds of abuse. They are directed, for instance, at determining whether indeed the person to be detected is in front of the recording apparatus rather than just a "copy", such as a photographic picture. In the case of facial recognition, for instance, attention can be paid to certain intrinsic movements within the face occurring during the recording, which would exclude the use of a photograph. It is evident that such safety measures are not invincible because the system might be outwitted by a video recording instead of a photograph.

It is even more difficult to protect biometrical data once they have been recorded. If an unauthorized person gets a hold of such a personal data record there is practically no chance of preventing that person from feeding the data illegally into an access data net and thus obtain acces to the system.

It is, therefore, an object of the instant invention to indicate a new method and system of biometrical identification of persons which offer better protection against forgery.

This object is met by a method comprising the features of claim 1 and a system comprising the features of claim 11.

The method and system according to the invention require the person to make a certain movement before, during, or after the personal data serving for the biometrical personal identification are detected. And it is verified whether the person actually made the movement before the identification of the person is continued. The invention thus utilizes an interactive method and system to guarantee that indeed a real user, namely the person wishing to obtain access to a protected area is located in front of the apparatus, rather than a copy.

In a first preferred embodiment of the invention a video camera is used to determine the position of the eyes and thus the line of sight of a person. For instance, any desired object is displayed on a screen and the person is asked to look at it. Detecting the position of the eyes can tell whether the person really looks in the given direction. By predetermining a plurality

of such randomly located objects and verifying whether the line of sight of the person changes in accordance with the positions of the object it can be made sure that there is a living person in front of the identification system and that what is entered is not a copy of the biometrical data set of the person.

In an alternative embodiment of the invention the position of a finger on a digitizer tray or the like may be detected instead of the position of the eyes. To do that, a mark may be displayed at different locations on the tray, and it may be sensed whether the user has placed his finger on the various positions of the mark.

Only after the user's motions under the direction of the system have correctly followed the predetermined positions, are the biometrical data (of the face, fingerprint or the like) as recorded by video or other detecting means, verified to see whether the user is an authorized person.

It is practically impossible with the method and system according to the invention to abuse a completed biometrical data set for a replay attack. The arbitrary positioning of objects whose movements the test person must follow makes it impossible for anyone but a real person actually present to pass the verification test. It is preferred to place a plurality of objects successively at different positions in order to exclude any coincidental agreement of the line of sight, hand position, or the like with the position of the object.

The invention will be described further, by way of preferred embodiments, with reference to the accompanying drawings, in which:

Fig. 1 is a flow diagram of a preferred embodiment of the method according to the invention; and

Fig. 2 is a schematic block diagram of the system according to the invention for biometrically identifying persons.

Fig. 1 shows a preferred embodiment of the method according to the invention.

In a first step 8, an error counter j is set to 0, and the number J of admissible false trials is fixed at 3, for example. In step 10, a test iteration counter n is set to 0, and the number N of test runs is fixed at 3, for instance. Any other suitable number may be chosen. In step 12, the video picture of a test person is recorded and stored in digital form. In step 14, thereupon, an

object is displayed on a screen at a random position, and the test person is asked to look at the object.

In step 16, the pair of eyes of the test person are sensed, i.e. video detected and transduced into digitized form, and the line of sight is determined. That may be accomplished by applying the method described in patent DE 19 632 237, for example.

In step 18, it is verified whether the line of sight of the test person is directed at the object displayed on the screen. Here, a certain time interval may be predetermined within which the line of sight must lie in the right direction. If that does not happen, the method returns via steps 32 and 34 to step 10 so that the setting of the iteration counter n will continue to be 0. The whole identifying procedure is started once more. In step 32, the error counter is incremented by 1 and, in step 34, it is checked if the line of sight has failed J (= 3) times to be directed towards the object displayed. If j < J renewed directing and detecting of the line of sight is started, in step 10. However, if J (= 3) mistrials already have been made the identification loop is left via an alarm stage 36. An operator or a program will be notified, who or which may then initiate appropriate measures.

If, on the other hand, the line of sight is directed at the object displayed on the screen the iteration counter n is incremented by 1, in step 20. In step 22, it is verified whether the iteration counter n has reached the maximum number N (= 3) of runs. If that is not the case the program returns to step 12 where again the picture of the test person is taken and memorized. Subsequently, the line of sight is verified in steps 14 to 18. During this run, and every consecutive one, the object always is shown at a different place on the screen.

Upon successful termination of the predetermined number of test runs, i.e. if in the present case n = N = 3, the safety check has been completed positively and, in step 24, the procedure continues with the biometrical identification which may take the course as described in patent application DE
19 847 261.

Fig. 2 is a greatly simplified illustration of the system according to the invention of identifying persons according to a preferred embodiment, including its fundamental elements. The system comprises a monitor 26, a camera 28, and a control and evaluator unit 30. An

object 32 is displayed on the monitor 26 at a randomly selectable position to direct the line of sight of a test person (not shown). A video picture of the test person, especially of the face of the test person or even more specifically of the eyes of the test person may be taken by the camera 28. The picture is digitized and processed in the control and evaluator unit 30 in accordance with the method described above.

It is a great advantage of the invention that it can be implemented with standard hardware, such as a conventional PC including a monitor and video camera. It does not require any special environment. The predetermination of a greater number of randomly selected object positions on the monitor allows any desired high level of security to be achieved.

As mentioned initially, it is possible, of course, to apply other biometrical methods of detection besides optically scanning a test person. For example, a fingerprint may be recorded by thermal, capacitive or other methods at different predeterminable positions on a display or detector screen.

In future, the method and system according to the invention may be used for automatic and biometrical access control. A procedure of verifying the line of sight of the eyes, the position of a finger, or the like either before, during, or after the identification procedure ensures that the personal identification indeed is effected on a living being. A comparison of the personal data resulting from that procedure with reference data guarantees that the person really is a desired or authorized individual.

The above merely describes the fundamentals of the invention without going into detail as regards per se known methods of biometrically identifying persons. Such methods are specified, for example, in patent application DE 19 847 261 to which reference was made above and also in the publications mentioned in that patent application. A person having average skill in the art will be able to select a method of identifying persons which is suitable for any specific application.

The features disclosed in the specification above, in the claims and drawings may be essential for implementing the invention in its various embodiments, both individually and in any combination desired.

DCS Dialog Communication Systems AG
D 2963 PCT

WHAT IS CLAIMED IS:

1. A method of securing forgery in biometrical identification of persons which includes detecting at least one biological characteristic of a person and transforming it into personal data (12) in order to recognize the person (24), characterized in that the person is caused (14) to carry out a controllable motion, and said motion is detected (16) to verify if the person is actually present.

2. The method as claimed in claim 1, characterized in that the line of sight of the person is controlled and the position of the eyes is detected.

3. The method as claimed in claim 2, characterized in that at least one mark is preset at a random position on a monitor, and it is detected whether the person's line of sight is directed to that mark.

4. The method as claimed in any one of the preceding claims, characterized in that the person is caused to place a hand or parts thereof at a predeterminable position on a biometrical detector means, and that biometrical data of the hand or parts thereof at this position are detected.

5. The method as claimed in any one of the preceding claims, characterized in that the person is caused to carry out similar motions repeatedly in succession, said motions being directed to different predeterminable positions.

6. The method as claimed in claim 5, characterized in that a first target direction is predetermined for the motion and it is checked whether a first motion follows the predetermined target direction, and at least one other target direction is predetermined which differs from the first target direction, and it is checked whether at least a second motion follows this other target direction, and the biological characteristic of the person is detected if at least the first and second motions follow the respective target directions.

7. The method as claimed in claim 5 or 6, characterized in that an alarm is given if the motions do not follow the target directions repeatedly in succession.

8. The method as claimed in any one of the preceding claims, characterized in that a facial picture is taken of the person and digitized, and the actual position of the eyes in the digitized image is detected and compared with a rated eye position, and the digitized facial image is compared with at least one digital facial reference image if the actual eye position largely corresponds with the rated eye position.

9. The method as claimed in any one of the preceding claims, characterized in that the picture of a hand print or finger print of the person is taken and digitized, the actual position of the picture in a detection area is determined and compared with a rated position, and the digitized image is com-pared with at least one digital reference image if the actual position largely corresponds with the rated position.

10. The method as claimed in any one of the preceding claims, characterized in that the motion is detected before, after, or during the identification of the person.

11. A system of securing forgery in biometrical identification of persons, comprising a detector means (28) for detecting at least one biological characteristic of a person and a processing means (30) for transforming the characteristic detected into personal data, **characterized** by a directing means (26) for releasing a certain motion of the person, the motion being detected by the detector means, wherein said processing means (30) verifies whether the person is actually present in dependence of the detection result.

12. The system as claimed in claim 11, characterized in that the directing means comprises a monitor (26) on which a mark is adapted to be displayed at random positions in order to direct the person's motion to that mark.

13. The system as claimed in claim 11 or 12, characterized in that the directing means (26) controls the person's line of sight, the detector means (28) detects the eye position, and the processing means (30) digitizes the eye position detected and compares it with the rated eye position.

14. The system as claimed in claim 11, characterized in that the directing means is part of the detector means.

15. The system as claimed in claim 14, characterized in that the detector means comprises a digitizing tray to control the person's hand motions and detect the position of the hand, and the processing means digitizes the hand position detected and compares it with a rated position.

16. The system as claimed in claim 14 or 15, characterized in that the detector means detects a fingerprint of the person at the rated position only.

17. A method of biometrical identification of persons, comprising a method as claimed in any one of claims 1 to 10, characterized in that the person's data are compared with reference data.

18. A means for biometrical identification of persons, comprising a system as claimed in any one of claims 11 to 16, characterized in that the processing means compares the person's data with reference data.

BioID AG
D2963US

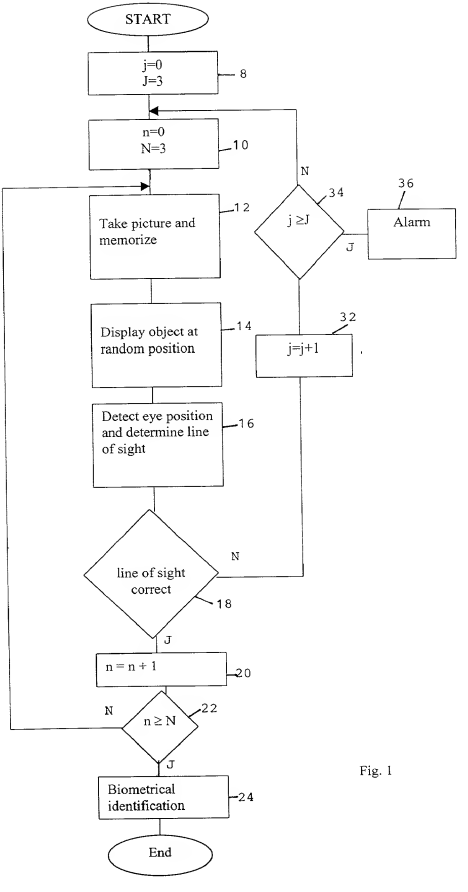

Fig. 1

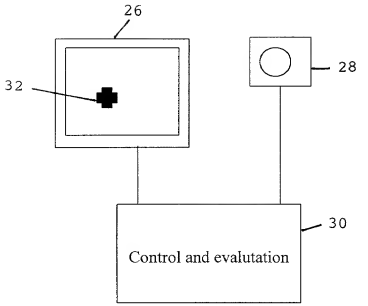

Fig. 2

ATTORNEY DOCKET NO. BOE01 003

COMBINED DECLARATION AND POWER OF ATTORNEY FOR UTILITY PATENT APPLICATION

As a below named inventor, I hereby declare:

that my residence, post office address and citizenship are as stated below next to my name;

that I verily believe that I am the original, first and sole inventor (if only one name is listed below) or a joint inventor (if plural inventors are named below) of the invention which is the subject of an application entitled: A METHOD AND SYSTEM OF SECURING FORGERY IN BIOMETRICAL IDENTIFICATION OF PERSONS; said invention being described and claimed [ ] in the attached specification [ ] in the specification of application Serial No. 09/889,600 ✓, filed July 19, 2001; that I have reviewed and understand the content of said specification including the claims; that I do not know and do not believe the said invention was ever known or used in the United States before my or our invention thereof, or patented or described in any printed publication in any country before my or our invention thereof or more than one year prior to said application; that said invention was not in public use or on sale in the United States more than one year prior to said application; that said invention has not been patented or made the subject of an inventor's certificate issued before the date of said application in any country foreign to the United States on an application filed by me or my legal representatives or assigns more than twelve months prior to said application; that I acknowledge my duty to disclose information of which I am aware which is material to patentability as defined in 37 CFR 1.56; and that no application for patent or inventor's certificate on this invention has been filed in any country foreign to the United States prior to said application by me or my legal representatives or assigns, except as follows:

COUNTRY/INTERNATIONAL	APPLICATION NUMBER	DATE OF FILING (day, month, year)	PRIORITY CLAIMED UNDER 35 U.S.C. 119/365
Germany ✓	DE 199 01 881.2 ✓	19.01.99 ✓	YES X NO
			YES NO

I hereby claim the benefit under 35 U.S.C. §119(e) of any United States provisional application listed below:

U.S. Provisional Application S.N. _____ filed _____.

I hereby appoint L. Lawton Rogers, III, Reg. No. 24,302; D. Joseph English, Reg. No. 42,514; Mark C. Comtois, Reg. No. 46,285; and Patrick D. McPherson, Reg. No. 46,255 to prosecute said application and to transact all business in the Patent and Trademark Office connected therewith and to file, prosecute and transact all business in connection with international applications directed to said invention:

Address all correspondence to: Carter, Ledyard & Milburn
1401 Eye Street, N.W., Suite 300
Washington, DC 20005

Address all telephone calls to (202) 898-1515

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

1-00 Robert Frischholz
FULL NAME OF SOLE OR FIRST INVENTOR

X [signature] 10/19/01
SIGNATURE DATE

Nordgaustr. 9, 90427 Nürnberg DEX
c/o Bilofa AG, Am Weichselgarten 10a, 91058 Erlangen
RESIDENCE

Germany ✓
CITIZENSHIP

Nordgaustrasse 9, 90427 Nürnberg
c/o Bilofa AG, Am Weichselgarten 10a, 91058 Erlangen
POST OFFICE ADDRESS

X
FULL NAME OF SECOND JOINT INVENTOR, IF ANY

SIGNATURE DATE

RESIDENCE

CITIZENSHIP

POST OFFICE ADDRESS

___ LIST OF ADDITIONAL INVENTORS ATTACHED